Comisario Inspector PABLO RAUL DE CRISTOBAL
Jefe Dpto. INVESTIGACIONES ADMINISTRATIVAS

POLICIA FEDERAL ARGENTINA FOLIO 74

DILIGENCIA: Constancia de la instrucción.

-///- Buenos Aires, Capital Federal de la Nación Argentina, hoy 26 de septiembre del año 2019, siendo la hora 18:15 la Instrucción hace constar: que se conformó el expediente IF-2019-73519914-APN-DIAD#PFA conteniendo informe procedente de la Sección CIBERSEGURIDAD, en el cual se resalta: "…Del análisis surge hasta el momento, esta Sección CIBERSEGURIDAD informa que no cuenta con información que permita determinar si en el ataque cibernético que sufrió la Institución se encontraría personal policial involucrado. En tanto las dependencias que sufrieron la fuga de información por acción del ciber delincuente y de acuerdo a los archivos que se lograron visualizar con las aplicaciones específicas desde la "Deep Web", se llegó a la conclusión que pertenecerían a las áreas de SUBJEFATURA, BIENESTAR, DROGAS PELIGROSAS, PERSONAL SUPERIOR E INTERIOR. Se informó que desde el día **12/8/19**, fecha en que se tomó conocimiento de la fuga de información institucional, se inició la descarga del contenido desde la "Deep Web" a una velocidad de transferencia muy baja, demandando más de veinte días en tratar de obtener la mayor cantidad de información posible. Pese al esfuerzo de esa Sección y de otras áreas específicas de esa Superintendencia, con fecha 2 de septiembre del corriente, se interrumpió la descarga por no encontrarse disponible la dirección de internet donde se había publicado, continuando a la fecha fuera de línea. Logrando obtener 500 gb de información.

Pormenores de los acontecimientos: Con fecha **12/8/19**, siendo las 10:40 horas se tomó conocimiento por intermedio del Sr. Director de CIBERCRIMEN del Ministerio de SEGURIDAD DE LA NACIÓN, que en la plataforma de la red social Twitter y posteriormente Telegram, mediante la cuenta @lagorraleaks, se efectuaron diversas publicaciones donde los ciber delincuentes habrían publicado en la red TOR (Deep Web), 700 GB de información de esta Institución. Ante tal magnitud, se conformó en el ámbito de la Sección CIBERSEGURIDAD un "Comité de Crisis", por el Sr. Superintendente FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, Director General de INTELIGENCIA CRIMINAL, Director General de OPERACIONES TÉCNICAS, Jefe Departamento TÉCNICO CONTRA EL NARCOTRÁFICO, Jefe Departamento TÉCNICO

OPERATIVO, Jefe A/C Departamento MOVIMIENTO DE PERSONAL, Director de INVESTIGACIONES CIBERCRIMEN de la Provincia de Buenos Aires, y Oficiales Jefes de las Distintas Áreas supuestamente alcanzadas. Posteriormente, y ya teniendo identificado el tipo de información filtrada, la Sección CIBERSEGURIDAD estableció en principio, que uno de los vectores de ataque correspondieron a la intrusión de los ciber delincuentes a diversas casillas de correos comerciales (Hotmail, gmail) utilizadas por las dependencias policiales, mediante una técnica de phishing que fuera detectada, reportada por esa Sección y mitigada con fecha 30/7/19, por la Sección INFORMÁTICA de la Superintendencia de BIENESTAR, en razón de que en el sitio de la Página Oficial http://supbienestar.gob.ar se encontraba alojado un formulario malicioso que simulaba ser de un acceso al servicio de Onedrive para la descarga de un archivo, técnica utilizada por el ciber delincuente para apoderarse de los nombres de usuarios y contraseñas de acceso, según se desprende de comunicaciones efectuada por dicha Sección. El Departamento CIBERDELITO, al tomar conocimiento de este tipo de técnica de phishing, judicializó la causa en la que interviniera el Juzgado en lo Criminal de Instrucción N° 6 a cargo de la Dra. María Alejandra PRIVITOLA, Secretaria N° 118 del Dr. Mariano FREIJO. Asimismo, con fecha **30/07/19**, la Sección efectuó las comunicaciones de estilo a la Superioridad y elaboró un Boletín Informativo N° 10, mediante el cual se explicó la maniobra de engaño, efectuando las recomendaciones del caso, como ser: El cambio urgente de contraseñas para las dependencias que pudieran haber ingresado al sitio malicioso y la obligatoriedad del uso del correo electrónico Institucional para garantizar la veracidad y confidencialidad de la información, entre otras, para conocimiento de la totalidad de las dependencias de la Institución. Una vez determinada en forma parcial la metodología de ataque empleada que ocasionara la fuga de información institucional, se advirtió a la totalidad de las áreas de la Institución, a través de la División GESTIÓN ADMINISTRATIVA de la amenaza en cuestión, con la finalidad de que la totalidad de las dependencias de cada área proceda en forma urgente al cambio de contraseña de las cuentas de correo electrónico, servicios de almacenamiento en la nube, conexiones WI-FI y cualquier otro dispositivo que precise credenciales para su acceso. En el mismo sentido, se retransmitió mediante la plataforma del Sistema de Mensajería Electrónica SAFWIN y correo electrónico Institucional,

Comisario Inspector PABLO RAUL DE CRISTOBAL
Jefe Dpto. INVESTIGACIONES ADMINISTRATIVAS

POLICIA FEDERAL ARGENTINA FOLIO 75

directivas con respecto a cambio de contraseñas de los servicios enunciados anteriormente, como así también en forma indefectible se proceda a la habilitación de un doble factor de autenticación para garantizar un acceso seguro. El **13/8/19**, a partir del análisis de la información obtenida hasta ese momento, y habiendo identificado algunas de las áreas afectadas por la fuga de datos, por disposición de la superioridad, se brindó una charla informativa y de concientización a la Plana Mayor de la Institución en el auditorio de la Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, donde se expusieron las técnicas de ataque, las áreas comprometidas, el tipo de información comprometida y el avance de las tareas de análisis que venía desarrollando la Sección CIBERSEGURIDAD.

REPUBLICA ARGENTINA POLICIA FEDERAL ARGENTINA DEPARTAMENTO INVESTIGACIONES ADMINISTRATIVAS

El día **14/8/19**, se conformó una reunión del COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, integrada por Oficiales Superiores y Jefes de las principales áreas específicas, donde se expuso entre los presentes los hechos de conocimiento público, a los fines de analizar la cuestión y realizar recomendaciones para mitigar estos sucesos. En esa inteligencia, el Comité elaboró un documento "Normas de Seguridad Informática" con reitero de objetivos inmediatos y a futuro que eviten la fuga de información Institucional.

Con fecha 15/8/19, el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN convocó a representantes de todas las áreas de la Policía Federal Argentina, en la que se puso en conocimiento de los avances y pormenores del ciber ataque, se instrumentó la designación de un oficial enlace permanente para transmitir o recibir comunicaciones vinculadas a la problemática en cuestión. También, se consolidaron los lineamientos de seguridad oportunamente comunicados, en especial el reitero de la prohibición del uso de cuentas de correo comerciales para el manejo de información institucional. Esa misma fecha, se enviaron comunicaciones oficiales por el sistema de gestión documental electrónica (GDE), informando a las Divisiones GESTIÓN ADMINISTRATIVA de todas las Superintendencias, a los efectos de advertir mediante listados de Excel embebido, cuáles eran las dependencias que fueron comprometidas, al mismo tiempo que se reiteraron las medidas de seguridad que deben implementar (backup, escaneos de malware, entre otras) con la finalidad de resguardar toda la

información de la dependencia y, en caso de ser necesario, se proceda a la contención del equipo informático aislándolo de la red e internet.

Posteriormente, con fecha viernes 16 de agosto se convocó a los representantes de cada superintendencia y se los puso en conocimiento de las directivas de buenas prácticas dispuestas por el Comité de SEGURIDAD DE LA INFORMACIÓN en lo relativo a las medidas a implementar en las distintas dependencias de esta Institución.

Con fecha 20 de agosto, por disposición del Sr. Superintendente FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, mediante comunicación a través de GDE, NO-2019-74615248-APN-SFTIYCDGA#PFA, comunica las "Normas de Seguridad Informática para su más estricto cumplimiento", entre las que se reitera el solo uso del correo electrónico Institucional bajo el dominio @policiafederal.gov.ar; la prohibición de almacenamiento de datos en la nube (OneDrive/Google Drive), entre otros.

Con fecha **22/08/19**, la Sección CIBERSEGURIDAD, tomó conocimiento de un ataque de malware tipo ransomware que involucro equipos informáticos de la Fiscalía de Estado Bonaerense, por lo que se procedió a realizar e informar mediante Boletín Informativo N° 13 a la totalidad de las áreas de la Institución, mediante correo electrónico y a través del sistema GDE.

El día **23/08/19**, la dependencia aludida, realizó un informe para concientizar al personal respecto a la amenaza de los ataques de ransomware y la forma de cómo prevenirlos.

El lunes **26/08/19**, 18:15 horas, se realizó en el Auditorio de esa Superintendencia, una reunión con los referentes técnicos de diversas áreas de la Institución vinculadas al tema, sumado a personal de la empresa de seguridad informática ESET; la cual se desarrolló en tres etapas.

1era Etapa: La Sección CIBERSEGURIDAD interiorizo a los presentes, de la magnitud de los acontecimientos recientes.

2da Etapa: Personal de la empresa ESET, describió el funcionamiento de sus soluciones que puedan mitigar estos tipos de amenazas y los beneficios que podría traer su implementación en los distintos sectores de la Institución.

Comisario Inspector PABLO RAUL DE CRISTOBAL
Jefe Dpto. INVESTIGACIONES ADMINISTRATIVAS

FOLIO 76

3ra Etapa: Se hizo un cierre de la reunión y se establecieron pautas de trabajo con respecto al desarrollo e implementación de Software, como así también, recomendaciones sobre la estructura de red de las distintas áreas.

Asimismo, el **27/08/19**, la Sección referida, dictó una academia alineada con la campaña de concientización que ya se venía realizando durante el año 2018 y 2019 al personal de esta Institución en sus distintos cuadros, Jerarquías y escalafones. Los temas tratados, fueron incluidos como temario obligatorio para la próxima academia que a nivel Institucional se realizan en todas las dependencias los últimos jueves de cada mes. Ese día, la División COMPUTACIÓN desarrolló y habilitó a través del portal PIPFA, una ventana emergente donde se dispone de algunas de las Normas de Seguridad Informática, para que de forma obligatoria la totalidad del personal de la Institución las lea y comprenda las mismas.

INSPECTOR DAMIAN MATIAS D'ANGELO
DEPARTAMENTO INVESTIGACIONES ADMINISTRATIVAS

Se dejó constancia que durante los años 2018 y 2019 se han dictado diferentes disertaciones, incluso se ha incorporado al "Plan Anual de Capacitación" dos cursos: "Introducción a la Seguridad de la Información", siendo realizado uno de ellos en el mes de marzo y otro en el mes de agosto del corriente, al cual han asistido representantes de diversas fuerzas federales. A raíz de lo sucedido se intensifico la cantidad de disertaciones, con el fin de que el personal tome conciencia de los riesgos a los que se está expuesto con el uso de las Tic´s y las distintas amenazas cibernéticas que cada día se vuelven más complejas con el avance de la tecnología.

FALLAS DE SEGURIDAD QUE POSIBILITAN DICHAS FILTRACIONES:

Para determinar a ciencia cierta cuales fueron las fallas que posibilitaron la fuga de información, se solicitó mediante sistema de GDE a las áreas de PERSONAL, DROGAS PELIGROSAS Y BIENESTAR a los efectos de que estas amplíen los motivos que dieran origen a la misma, por ser las dependencias propietarias de los datos personales filtrados, mediante NO-2019-75852101-APN-SCIB#PFA.

Se aclaró que la información que fuera afectada NO corresponde a datos de las bases que concentra los principales servicios informáticos que utiliza la Institución, las cuales se encuentran almacenadas en Servidores del Centro de Cómputos de la División COMPUTACIÓN, sino que pertenecen a datos descentralizados administrados localmente por

las áreas anteriormente mencionadas. Según se desprende de lo informado por la Superintendencia de BIENESTAR, a través de la Sección INFORMÁTICA mediante NO-2019-73090818-APN-SINF#PFA que textualmente refiere: …"El día 31 de julio del corriente año se tomó conocimiento a través de un llamado telefónico del Subcrio VITTUZI, Jefe de la Sección CIBERSEGURIDAD, de un e-mail enviado de la casilla div.supbienestar@hotmail.com (ajena a esta superintendencia) invitando a los usuarios a ingresar y completar un formulario alojado en nuestra web www.supbienestar.gob.ar, con el fin de descargar un archivo. El mismo trataba de un formulario fraudulento que simulaba ser el login de One Drive. Inmediatamente se procedió a eliminarlo de nuestra página ya que se comprobó que estaba recopilando correos y contraseñas en forma malintencionada. El día 12/8 se nos alertó de "hacker" que había publicado información personal de los afiliados de esta Policía Federal en la Deep Web. Se corroboro de donde provenía dicha información, tratándose de datos del personal que se obtuvo en formato .pdf de los afiliados de la obra social, realizada mediante un sistema de consulta que fue desarrollado por esa Sección (http://portal.supbienestar.gob.ar/gestion_angel). El mismo se encuentra publicado con el fin de que los anexos del interior puedan consultar el padrón y desempeñar sus funciones en base a esto, solo funciona a modo informativo, es decir, no posee permisos de escritura ni modificación sobre el padrón. Esa descarga, no se realizó a la fuerza si no que, por el contrario, el ingreso se estableció con usuario y contraseña validos dentro del mismo, las descargas comenzaron el 12 de agosto de 2019 a las 01:15 am en adelante desde la ip de origen 93.188. que se encuentra asignada al proveedor Hostinger International y a su vez la ip se localizó en la ciudad de Greenville de Carolina del Sur (EUA). Por otra parte se habían publicado contraseñas de muchos mails institucionales de esa superintendencia, concluyendo que la información fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmamil. Se estableció que se aprovechó de la información obtenida para poder conseguir acceso a mencionado portal del cual se obtuvo la información publicada.

Por su parte, la Superintendencia Federal de DROGAS PELIGROSAS, a través del Departamento SISTEMAS CONTRA EL NARCOTRÁFICO, respecto a las fallas que

Comisario Inspector PABLO RAUL DE CRISTOBAL
Jefe Dpto. INVESTIGACIONES ADMINISTRATIVAS

POLICIA FEDERAL ARGENTINA FOLIO 77

posibilitaron dichas filtraciones, informó: a) No se cuenta con recursos técnicos y humanos con capacidad para determinar dicha solicitud, b) Se desconocen la totalidad de datos filtrados, tipo y cantidad, por ende no se puede determinar que se hayan obtenido de esta Superintendencia. Respecto a la política de seguridad aplicada, se efectuaron: cambio de contraseñas cada determinado tiempo; cambio de clave de wifi; se promovieron diferentes charlas con el personal a fin que tomen conocimiento sobre los peligros de abrir correos no deseados o links que deriven a páginas web desde mails ya sean conocidos o no; se realizan backup periódicos de la información sensible; para comunicaciones Institucionales se utiliza únicamente el correo de POLICIA FEDERAL bajo el dominio (@policía federal.gov.ar). Se prohíbe el uso de cualquier otro correo. El correo Institucional se encuentra alojado en servidores de esta Institución y se encuentra segurizado mediante doble validación; la información sensible institucional, judicial y de los Recursos Humanos de estar almacenada en forma SEGURA (encriptada y con contraseña) en las computadoras y/o servidores de las Áreas y Dependencias. Reunida parte de la información y de acuerdo a las intervenciones del personal técnico de esa Sección, visualizando la información subida por los ciber delincuentes a la internet profunda (Deep Web) se puede concluir que las fallas que posibilitaron la filtración de los datos, son atribuidas en un principio al aprovechamiento y explotación de una vulnerabilidad del servidor web administrado por el área de Bienestar lo que ocasionara el alojamiento de un formulario malicioso para ser utilizado mediante la técnica de ingeniería social (phishing) y obtener las credenciales de acceso a las cuentas de correo no institucionales utilizadas por las dependencias de esta Institución y el robo de las fichas de formato PDF de los afiliados a la obra social. Como segundo factor, se debió a una falla humana por parte de los operadores de las cuentas no institucionales que fueran alcanzadas por el correo phishing y que permitió al ciberdelicuente obtener acceso total al servicio de correo tanto de Gmail y Hotmail y la descarga de la información que cada cuenta tenia almacenada en la nube, como ser servicio OneDrive y GoogleDrive, que involucra a Dependencias del área de SUBJEFATURA, Superintendencias Federal de DROGAS PELIGROSAS, PERSONAL, INSTRUCCIÓN Y DERECHOS HUMANOS y AGENCIAS Y DELEGACIONES FEDERALES. Y como tercer factor de ataque, tras el análisis de esta Sección

REPUBLICA ARGENTINA POLICIA FEDERAL ARGENTINA DEPARTAMENTO INVESTIGACIONES ADMINISTRATIVAS

INSPECTOR DANIAS DIANGELO
EPARTAMENTO INVESTIGACIONES ADMINISTRATIVAS

CIBERSEGURIDAD de los archivos de la Depp Web, se determinó que gran parte de los archivos que se filtraron corresponde a información almacenada en tres terminales informáticas utilizadas por la División PERSONAL SUPERIOR, las cuales pudieron haber sido comprometidas por el Ciberdelincuente con una infección de malware que permitiera el acceso total a los datos allí alojados en los discos rígidos, ya que se corroboro que esa Dependencia no utilizaba el almacenamiento de datos en la nube.

TIPO Y CANTIDAD DE DATOS PERSONALES QUE FUERON COMPROMETIDOS

El área de Bienestar informó: los datos comprometidos fueron: FICHAS PERSONALES DE LOS AFILIADOS, los cuales contienen los siguientes datos DNI, APELLIDO Y NOMBRE, N° AFILIADO, SEXO, ESTADO CIVIL, FECHA DE NACIMIENTO, EDAD, TELÉFONO FIJO Y MÓVIL, EMAIL, DIRECCIÓN, JERARQUÍA, SITUACIÓN DE REVISTA, LEGAJO PERSONAL, DEPENDENCIA, CBU, N° DE CAJA DE RETIRO, correspondiente a 220 mil fichas. Asimismo, se divulgaron 1083 cuentas de correo electrónico bajo el dominio @supbienestar.gob.ar con sus respectivas contraseñas.

Asimismo, se hizo saber que la Sección CIBERSEGURIDAD, no ha podido descargar para su análisis la totalidad de la información filtrada en la Deep Web, debido a que la tasa de transferencia para descarga es muy baja. No obstante, de lo que se desprende de lo visualizado existen gran cantidad de archivos de uso interno y administrativo de distintas dependencias que tuviera almacenados en los servicios de almacenamiento en la nube y los propios en discos rígidos internos ya anteriormente explicados. En relación con información con contenido de datos personales, ampliando lo informado por el área de Bienestar, se observa que, la carpeta identificada en la Deep Web como "DIVISIÓN DROGAS ESCUCHAS", se hizo un muestreo y se verifico la filtración de 39 fichas con datos y fotos del personal de esa Superintendencia. Respecto a datos con imágenes foto carnet 4x4 de uniforme para uso credencial; DNI escaneado de oficiales en condiciones de ascenso del año 2017; escaneo N° de control credenciales de grado; bases de datos del año 2017 con usuarios y contraseñas sistema "PERSUP"; audios de juntas ascenso, entre otros se encuentran en la carpeta "PERSONAL

78

SUPERIOR, DNI AGENTES, FOTOS DE PERFIL, AUDIO DE JUNTA, BACKUP BASE DE DATOS" del área de personal, hasta el momento no se puede determinar cantidad exacta de los datos filtrados. En ese sentido se adjuntó captura de pantalla de los directorios que se subieron en la "Deep Web", como así también listado de las cuentas que fueron víctimas de la técnica de phishing y sufrieron el robo de sus credenciales….". Se aguarda contar con la información que fuera infiltrada en el área de la Superintendencia de PERSONAL, INSTRUCCIÓN Y DERECHOS HUMANOS, en virtud de no haber sido informado por la División PERSONAL SUPERIOR, a la fecha de realizado el expediente en analisis. CONSTE

Comisario Inspector PABLO RAUL DE CRISTOBAL
Jefe Dpto. INVESTIGACIONES ADMINISTRATIVAS

INSPECTOR DAMIAN MATIAS D'ANGELO
DEPARTAMENTO INVESTIGACIONES ADMINISTRATIVAS